2010-06

Homeland Security Advisory System : an assessment of its ability to formulate a risk message

Ryczek, Martin E.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

HOMELAND SECURITY ADVISORY SYSTEM: AN ASSESSMENT OF ITS ABILITY TO FORMULATE A RISK MESSAGE

by

Martin E. Ryczek

June 2010

Thesis Advisor:	David Tucker
Second Reader:	Lauren Fernandez

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2010	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Homeland Security Advisory System: An Assessment of Its Ability to Formulate a Risk Message			**5. FUNDING NUMBERS**
6. AUTHOR(S) Martin E. Ryczek			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ________________.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unliminted			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The Homeland Security Advisory System was conceived in 2003. Within seven years, the system has become marginalized, even though the country continues to be at war with the forces of terrorism. The reason for this is that the system as designed does not allow for the successful crafting of a complete warning message. A warning message needs to be specific enough to allow the warning recipient to make the appropriate linkages between the warning message and the physical and social manifestations of the threat. This linkage allows the recipient to form his own unique risk reality. Once that is formed, the recipient may be motivated to take appropriate precautions to counter the threat. A warning message that does not allow for the formation of a risk reality can never be effective because the recipient will fail to internalize the risk and thus fail to take the appropriate action to counter the threat.

14. SUBJECT TERMS Homeland Security Advisory System, Risk Communication, Self Verification of Risk, Risk Reality, Risk Predictors, Hazard Characteristics.			**15. NUMBER OF PAGES** 61
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

HOMELAND SECURITY ADVISORY SYSTEM: AN ASSESSMENT OF ITS ABILITY TO FORMULATE A RISK MESSAGE

Martin E. Ryczek
Captain, Chicago Police Department, Chicago, Illinois
B.S., Illinois State University, 1983
M.P.H., University of Illinois, 1987

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
June 2010

Author: Martin E. Ryczek

Approved by: David Tucker
Thesis Advisor

Lauren Fernandez
Second Reader

Harold A. Trinkunas, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Homeland Security Advisory System was conceived in 2003. Within seven years, the system has become marginalized, even though the country continues to be at war with the forces of terrorism. The reason for this is that the system as designed does not allow for the successful crafting of a complete warning message. A warning message needs to be specific enough to allow the warning recipient to make the appropriate linkages between the warning message and the physical and social manifestations of the threat. This linkage allows the recipient to form his own unique risk reality. Once that is formed, the recipient may be motivated to take appropriate precautions to counter the threat. A warning message that does not allow for the formation of a risk reality can never be effective because the recipient will fail to internalize the risk and thus fail to take the appropriate action to counter the threat.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank Superintendent Jody P. Weis and Assistant Deputy Superintendent Theodore F. O'Keefe of the Chicago Police Department for allowing me the opportunity to enroll and attend the Master's Program of the Center for Homeland Defense and Security at the Naval Postgraduate School.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The purpose of this thesis is to examine whether the current Homeland Security Advisory System (HSAS) can successfully formulate a risk message to communicate the warning of a terrorist attack, and if it cannot, what action in regards to the HSAS should be taken by the Secretary for Homeland Security. Risk communication is defined as communication intended to supply the recipient with the necessary information to make informed, independent judgments about risks to health, safety, and the environment (Morgan, Fischhoff, Bostrom, & Atman, 2002, p. 4), an important part of all warning systems.

The HSAS was implemented in March of 2002. It was designed as a system to quickly inform the nation about dangers from terrorism threats. The system as implemented is a five-color-coded advisory system. Each color corresponds to a level of threat. The higher the threat condition; the greater the risk of a terrorist attack. The five threat conditions and their associated colors are as follows: Low = Green, Guarded = Blue, Elevated = Yellow, High = Orange and Severe = Red. Each threat condition is associated with specific protective measures to be enacted (see Appendix A). The threat system is binding on the executive branch of the federal government and voluntary for all other levels of government and the private sector (Homeland Security Presidential Directive 3, 2003). The system allowed the Secretary for Homeland Security to issue a warning for either the entire country or a specific geographical region based upon the threat intelligence received. In its early years, HSAS warnings were issued solely on a national basis; the HSAS did not issue any warnings on a regional basis until 2004 (see Appendix B).

A. CONTROVERSIES AND CRITICISMS OF THE CURRENT HOMELAND SECURITY THREAT ADVISORY SYSTEM

1. Initial Comments on Homeland Security Advisory System at Inception

The Homeland Security Advisory System was born in controversy and criticism. In its debut in May of 2002, the public-comment period produced 652 comments

regarding its initial design and implementation. A breakdown of the comments received placed them into five specific categories: Alert Status, Color Coding, Basic Design, Other, and Service (Federal Bureau of Investigation [FBI], 2002). The main issues for each of the categories are detailed in the chart below.

Table 1. Issues Produced in Public Comment Period

Category	Percent of Responses Citing Issue	Main Issue
Alert Status	34%	How the alert was to be disseminated.
Color Coding	20%	Colors chosen and the possibility that some individuals would not be able to differentiate between the colors.
Basic Design	21%	Refining the system to be more like NOAA weather watches and warnings; procedures to follow as threat levels rose.
Other	14%	Implications for 911 providers as threat levels were raised.
Service	11%	Training, support, and informational services.

2. Task Force Review of Homeland Security Advisory System

In 2009, Department of Homeland Security Secretary Napolitano convened a task force[1] to review the HSAS. A review of governmental reports, academic readings, and position papers on the threat system was compiled for the task force. This review revealed thirteen major issues reported upon since the system was implemented. The following issues were identified:

1. Vagueness of the system;
2. Loss of trust;
3. Lack of information sharing with state, local and private sector;
4. Incomplete warning system;
5. Failure to effectively communicate the threat;
6. Lack of specific protective measures;

[1] The task force members were Fran Townsend (co-chair), William Webster (co-chair), Randy Beardsworth, Richard Ben-Veniste, Matt Bettenhausen, David Bradley, James Carafano, Manny Diaz, Clark Ervin, Mary Fetchet, Shirley Franklin, Rick Fuentes, George Gascon, Christine Gregoire, Michael Rounds, Joe Shirley, and Ed Skyler.

7. Costs;

8. DHS training;

9. Better use of technology/news media;

10. System cries wolf;

11. Fear consumption for political gain;[2]

12. Lack of coordination between HSAS and other warning systems;

13. Too many colors (McQuillan, Nye, Munoz, & Mendelson, 2009).

The Task-Force report concluded that there was a disturbing lack of confidence in the HSAS (Homeland Security Advisory System [HSAS], 2009, p.1). In regards to risk communication, the task force made three specific recommendations. The first recommendation was for region specific rather than national warnings. The second, to provide as much threat detail consistent with national security along with a focus on the specific location/sector at actual risk. The last recommendation was for a return to normalcy as soon as practical (HSAS, 2009, p. 3).

3. The National Exercise Program

The National Exercise Program three times identified issues within the threat advisory system. In 2003, DHS released its After Action Report on Top-Off 2. This report recommended that the advisory system be further developed and synchronized with federal, state, and local governmental agencies in order to coordinate security enhancements. It was suggested that a coalition of federal, state, and local agencies develop an operational response and framework that could define response plans as threat levels changed (United States Department of Homeland Security [DHS], 2003, p.3). In Top-Off 3, the same findings and recommendations were made (DHS, 2005, p. 30). The AAR report on Top-Off 4 also concluded that the purpose, definitions, and consequences of the HSAS remained unclear (DHS, 2009, p. 10).

[2] Accusations have been made that HSAS threat levels have been raised solely to further political agendas. See Chapter II.

4. The Gilmore Commission

The Gilmore Commission (2003, p. 27) made three specific recommendations for the Homeland Security Threat Advisory system. The first was that the HSAS should issue warnings on a more regional basis in order to better define the exact area of the country directly impacted. The second recommendation was that the HSAS should provide training to emergency-response personnel to combat the expected threat. Lastly, it called for the issuance of specific guidance on security measures that should be enacted as the threat level changed.

These recommendations were based upon the fact that the commission felt that the threat system had become marginalized. This reason for this as cited by the commission was a lack of understanding of the use of the system and the absence of a well orchestrated plan to guide implementation of enhanced security measures at all levels (Gilmore Commission, 2003, p. 27).

5. United States General Accounting Office (GAO) Reports

The General Accounting Office also documented numerous issues concerning the HSAS; to date, it has produced ten reports for six different congressional committees. The time range of these reports is from early 2002 to July 2008. Two main concerns were raised in these reports: The first concern was for a revision to the HSAS to do away with the vague blanket system of warnings that was in use at its inception. The other concern was how to instill across this country a greater level of vigilance, preparedness, and readiness for all levels of government and the private sector.

In its report issued March 16, 2004, the GAO took a hard look at risk communication as it related to the Homeland Security Advisory System. In its report, "Risk Communication Principles May Assist in Refinement of the Homeland Security Advisory System," the GAO noted that warning systems should include consistent, accurate, and clear information on the threat at hand, including the time frame and affected locations (United States General Accounting Office [GAO], 2004, p. 1). It also stated that without adequate threat information, the public may ignore the threat or

engage in inappropriate actions, some of which may compromise rather than promote public safety. The following seven points were highlighted for specific improvements of the system:

1. Public warnings disseminated during heightened threat levels should provide specific, consistent, accurate, and clear information on the threat. including location and time (p. 2);
2. Federal, state, and local governmental units should be provided with better information (p. 2);
3. Call for communication protocols for the dissemination of warnings (p. 7);
4. The nature, timing, and extent of warnings must be considered (p. 8);
5. Publicly released information walks a thin line between too much and too little detail; either can cause unnecessary worry or apathy depending on the situation (p. 10);
6. The lack of information coupled with a false warning make the HSAS lose credibility (p. 14);
7. Specific threat information to be released during threat advisories (p. 18);

These points remain unresolved today.

B. PROBLEM STATEMENT

The Homeland Security Advisory System (HSAS) was announced to the nation on March 11, 2002 in Homeland Security Presidential Directive 3 (2003). The intent of this system was to create a common vocabulary, context, and structure for an ongoing national discussion about the nature of threats that confronted the homeland and the appropriate security responses that could be put in place to counter those threats. As noted above, numerous governmental reports and studies have cited deficiencies within the advisory system. The system as currently designed fails to instill confidence within its recipient audience as to its ability to forewarn of terrorist activity.

Both the Napolitano task force and the GAO noted this issue. The task force viewed with concern the vulnerabilities associated with the current advisory system. The very first concern they cited in their report was an erosion of public confidence in and

respect for the HSAS (2009, p. 5). The GAO noted, "It is not the number of perceived false alarms that will cause the public to ignore future warnings and develop a sense of complacency about the hazard; rather it is the lack of information provided to the public regarding the perceived false alarm that will cause the warning system to lose its credibility" (GAO, 2004, p. 14).

C. RESEARCH QUESTION

Why has the nation's terror threat warning system become irrelevant in less than a decade even though the nation continues to be at war with the forces of terrorism? The answer to this question lies within the ability of the HSAS to communicate risk. As noted above, risk communication is defined as communication intended to supply an audience with the information it needs to make informed, independent judgments about risks to health, safety, and the environment (Morgan et al. 2002, p. 4). Effective risk communication concentrates on the information that recipients need the most in order to understand that risk. This thesis looks at the ability of the HSAS to adequately communicate that risk.

D. PRACTICAL SIGNIFICANCE OF THE RESEARCH

The results of this research will show that the current design of the HSAS does not sufficiently provide the essential informational elements required for effective risk communication. Audiences must not only have the ability to hear the risk message that is being disseminated, they must also receive the proper information in sufficient detail to allow them to make linkages between the warning message they receive and the physical manifestations of the threat (see Chapter II, Section C, Item 4a). It is these linkages that allow recipients to internalize the risk message by forming their own unique risk reality. Once the recipient forms this risk reality, he may then be motivated to the point of taking protective action. Warning messages that do not provide sufficient detail to allow for this internalization process can never hope to be effective. Once having identified these informational shortcomings within the HSAS, a recommendation can be made for the Secretary of Homeland Security as to the most prudent course of action.

E. LIMITATIONS OF THE RESEARCH

This thesis looks at the ability of the HSAS to supply the relevant information needed in sufficient quantity to allow for a proper risk communication message to be drafted. This thesis will not look at the actual crafting of the risk message,[3] the message communication medium or recipient audiences; these areas have been extensively examined by others. (See, e.g., call-to-action (Smith & Piltz, 1999; Sharp, Blottman, & Troutman, 2000; Smith, 2000); message communications medium (Rogers & Sorensen, 1993); and receptor audiences (Perry & Mushkatel, 1986; Quarantelli & Taylor, 1977)).

F. COMMON TERMS

For purposes of this thesis, the recipient for a risk communication may be a governmental agency, private entity, or an individual. Other terms that will be used throughout will be "risk prediction," "hazard characteristics," and "independent self-verification of risk." Risk prediction and hazard characteristics are the two sets of essential informational elements required for proper crafting of the risk message. Risk prediction is the ability to adequately define the following in advance of event onset: time frame, location, level of certainty, along with an estimate of magnitude and consequence. Hazard characteristics further refine the event in terms of its certainty, detectability, predictability, visibility, and duration of impact. Independent self-verification of risk is the ability of the recipient to link the warning message to a physical characteristic of the risk that can be experienced through sight, touch, or social affirmation.

G. METHODOLOGY

1. Overview

This thesis will examine the HSAS in relation to its ability to supply the essential informational elements to allow for a proper risk communication message to be drafted. A comparative analysis will be made between the HSAS and three other warning systems in order to measure the individual abilities of each to supply the essential informational

[3] The National Weather Service refers to these as "call to action" statements.

elements. A numerical comparison will then be made between the different warning systems and the HSAS in order to compare its effectiveness in communicating risk.

2. Comparative Analysis

The warning systems that the HSAS will be compared against are the National Fire Danger Rating System Description (National Weather Service) for forest fire prevention, and the National Weather Service's tornado and hurricane warning systems. The thesis will first provide an overview of how each of these warning systems meets the basic requirements of an effective system: detection, emergency management, and public response (Mileti & Sorensen, 1990). Second, it will look at how the essential informational elements play a role in the independent self-verification of risk by the recipient. The last step in the comparison will evaluate these warning systems against the five factors for risk prediction and the six hazard characteristics identified as being essential informational elements for a successful warning system. A numerical summation of these factors will be used to make an overall judgment on the effectiveness of the HSAS to supply the needed informational elements to adequately communicate risk. The five factors for risk prediction and the six hazard characteristics are drawn from a study on warning systems by the Oak Ridge National Laboratory.

Chapter II provides information on why we have warning systems, along with a comparison of the different warning systems. Chapter III analyzes the several systems. Chapter IV provides a recommendation to the Secretary of Homeland Security regarding the continued use of the HSAS.

II. COMPARISON OF WARNING SYSTEMS

A. WHY WE HAVE WARNING SYSTEMS

1. Executive Order 13407

President Bush signed Executive Order 13407 on June 26, 2006. This Executive Order states:

> It is the policy of the United States to have an effective, reliable, integrated, flexible, and comprehensive system to alert and warn the American people in situations of war, terrorist attack, natural disaster, or other hazards of public safety and well being (public alert and warning system), taking appropriate account of the function, capabilities, and needs of the private sector and of all levels of government in our Federal system, and to ensure that under all conditions the President can communicate with the American people.

Our country is a technological nation. We use our technology to build safer structures, but we cannot completely safeguard ourselves from the destructive forces of nature or man. As the Oak Ridge National Laboratory Report states: “Warning systems are used as our last line of defense after engineered solutions are applied to reduce the probability of an event below an acceptable standard.” (Mileti & Sorensen, 1990, p. 1–1) Further, “warning systems are economically rational only when risk becomes an actual event and when having inadequate or no warning system is politically and socially unacceptable” (Mileti & Sorensen, 1990, p. 1–1).

A report prepared by the General Accounting Office to the Subcommittee on National Security Emerging Threats and International Relations stated: “A well thought out and developed early warning system not only assists in prevention but also in implementing action to reduce vulnerabilities and preparation for enhanced response and recovery. ” (GAO, 2004)

2. Other Types of Warning Systems

As a nation, we strive to keep our citizens informed, so they can make rational choices regarding the amount of risk they are willing to accept under a specific set of

circumstances. A logical extension of this idea is the creation of different types of warning systems. One of the most effective warning systems, and the most familiar, is the National Oceanic and Atmospheric Administration's National Weather Service (NWS) system of weather watches and warnings. This warning system is used almost every day throughout the country. The NWS system has saved countless lives and reduced property losses (United States National Committee for the Decade for Natural Disaster Reduction [U.S. National Committee], 1991, p. 37). However, this is not our only warning system; the nation has many other different types of warning systems. There are systems that warn of technological disasters (i.e., hazardous material spills, nuclear materials releases), geological events (i.e., earthquakes, volcanoes), climatological events (i.e., tornados, hurricanes, and blizzards), and man-made events (i.e., missile attacks, air raids) (Mileti & Sorensen, 1990, p. 1-2). Warning systems are communication tools for government to quickly communicate with audiences about the dangers they face. In Chapter III, a comparative analysis will be made between the HSAS and three other warning systems. The purpose of the comparison is to measure the ability of the different systems to supply the essential informational elements necessary for risk communication.

B. BASIC PRINCIPLES OF RISK COMMUNICATION

The basic principles of risk communication used in all of these warning systems are twofold; the first is to supply recipients with sufficient information so they are able to adequately prepare for the coming threat. The other is to avoid giving an undo assurance of safety and security. Thus, the information provided must strike a balance between too little and too much. The GAO report on Risk Communication Principles states that too much information on a threat could result in public panic and disorganization, while too little information could result in public denial, apathy, and inaction (GAO, 2004, p. 10). The recipients must be able to understand not only the nature of the threat but the appropriate measures they can take to reduce their own vulnerabilities in conjunction with others to try and prevent the occurrence or lessen its impact. Warnings communicate to the community at large the nature of the threat and the level of precautions to be taken. For these reasons public alerts must be credible, specific, understandable, and actionable by the recipients (Tierney, Lindell, & Perry, 2001, p. 30).

C. HOW AN EFFECTIVE WARNING SYSTEM WORKS

The focus of this thesis is to define whether or not the HSAS has the ability to supply a sufficient amount of the essential informational elements to construct a risk communication message. The comparison will be made by using the identified risk predictors and hazard characteristics as identified in the Oak Ridge National Laboratory study entitled, "Communication of Emergency Public Warnings, A Social Science Perspective and State-of-Art Assessment."[4] This study defines the structure for an effective warning system as having three distinct subsystems: detection, emergency management, and public response. Within each of these three subsystems, the individual components needed to effectively communicate the risk to the appropriate audience were assessed. As to detection, the study examined the factors of monitoring, data assessment and analysis, prediction, and information conveyance. Within emergency Management, it examined the relevant factors of interpretation, decision to warn, methods and content of warnings, and monitoring of the response. Lastly, in the public response subsystem, the factors of interpretation, response, and informal warnings through social interaction were examined. [5] In order to fully understand the comparison in Chapter III, we must first detail how the pieces of an effective warning system work.

Detection is the ability to discover an event before onset. This is the key to an effective warning system because if the event is not discoverable before onset, there is no reason to have a warning system. Emergency management describes how government and the private sector prepare for the event. While the actions to be taken may vary, it is the ability to preplan for the event and then to begin implementation of the plan before onset that makes the emergency management subsystem effective. The implementation of a plan before event onset allows us to lessen the impact and severity of the event. The

---

[4] The Oak Ridge National Laboratory Study was chosen for use in this thesis because of its extensive investigation into the relevant social factors that make risk communication effective. This work builds upon an earlier work, *The Warning System in Disaster Situations: A Selective Analysis* by McLuckie (1970). In the Oak Ridge National Laboratory Study, the authors researched over 200 other studies that investigated warning systems and warning responses. The study has been cited repeatedly since its publication. As of January 2010, the Oak Ridge study has been cited in 84 other scholarly publications.

[5] For this thesis public response is identified as the appropriate recipient audience, be it a governmental agency, a private entity, or an individual

third and last subsystem is public response, the ability of the recipient audience to not only hear the warning but understand it sufficiently so that it can internalize the threat. The internalization of the threat process may then in turn motivate the receptor to take protective actions to safeguard himself and others.

Throughout the rest of this section, I will use the examples of forest fire prevention, along with tornado and hurricane warnings, to demonstrate briefly how two of these subsystems (detection and public response) relate to the overall effectiveness of a warning system. The HSAS is subject to criticism because it does not effectively relate to these subsystems because it lacks risk-predictor and hazard-characteristics informational elements. Since the focus of this thesis is to determine whether the Homeland Security Advisory System (HSAS) has the ability to communicate the risk of a terrorist attack, I will not address the issue of emergency management as it relates to HSAS warnings.

1. Detection

In the case of forest fire prevention, a color-coded scale is used to inform about conditions within a specific geographical forest area. The color codes used are: green, blue, yellow, orange, and red. These colors represent the susceptibility of a specific forest to unplanned ignition. Predictions for the possibility of unplanned ignition are based on terrain, the amount of ground cover, the moisture in the ground cover, the expected ambient temperatures over a defined time period, and the expectation of moisture (rain). These factors are combined through modeling to provide a realistic prediction for unplanned ignition (Faculty of Forestry). The major component that makes this part of the system effective is that there are very specific, definable parameters, and as these change, the warning level can be adjusted as warranted.

In the case of tornado warnings, science again plays a major role with thunderstorm detection through the use of radar and satellite imaging. Since thunderstorms are the precursors to tornados, once a thunderstorm is detected, the movement and intensity of the storm can be defined and plotted. Judgments can then be made for the potential of the thunderstorm to spin off tornados (Klemp, 1987, pp. 369–402). This system is employed numerous times a year with a defined cycle of event

detection (thunderstorm) followed by the issuance of tornado watches and warnings. Although every thunderstorm does not produce a tornado, the arrival of the thunderstorm signals the probability within a level of certainty for event onset.

In the hurricane warning scenario, science again plays its part through satellite imaging. Satellites allow us to see tropical storm formation and its progression into a hurricane while it is well out over the ocean (Katsaros, Forde, Chang, & Liu, 2001, pp. 1043–46). This allows for very specific hurricane prediction—sometimes days before it ever impacts a land area. As the hurricane nears the shores of our nation, revisions in the warnings forecast the exact location and intensity.

Detection of terrorist intent can lead to HSAS warnings. “Detection,” however, is not a scientific endeavor as it relates to terrorism; rather, it is based upon the collection of classified intelligence data that often requires skilled analysis to make relationships out of seemingly unrelated pieces of information. Detecting a terrorist event is an imprecise science at best and one that the public in general is not normally allowed to access. This is not to say, however, that we have no ability to foretell of an impending attack. On occasion we do uncover terrorist plots. When this happens, however, warnings do not always come into play because law enforcement is often able to successfully interdict the plot long before the need for a warning arises. Likewise, the warning itself, once issued, might deter the terrorists from plot execution (warnings in the other systems can never achieve this).

The HSAS does have credibility issues as to its ability to forewarn; since its inception in March of 2002, it has placed the nation on a heightened level of alert (yellow). On nine separate occasions, the HSAS has been upgraded to orange. The criticisms here as noted by both the GAO and the Napolitano task force is that the system has cried wolf and raised the threat level, but no terrorist event has ever taken place, nor was an intervention action ever publicly announced that linked the increase in the HSAS threat warning and the claim of the government that it can detect a terrorist event before onset. Additionally, no acknowledgment has ever been publicly documented that the

issuance or increase in the warning either deterred or prevented a terrorist attack from occurring. Thus, there is no public evidence that the nation has any ability to detect and then appropriately warn of a terrorist-sponsored event before onset.

2. Public Response

Harold E. Brooks and Charles A. Doswell (2001, p. 360) cite an example of how a warning system may contribute to public safety. According to these authors, deaths due to tornados have been decreasing since 1925 from 1.8 per million population per year to 0.12 per million per year in 2000. Although they attribute the decline to a variety of factors, they cite warnings as a contributing factor. As noted earlier, this thesis does not explore the transmission method of the risk message or the factors that influence the ability of the audience to understand the message and subsequently internalize the threat that might motivate them into action.

3. Independent Self-Verification of Risk

a. Internalization of Risk Message

Independent self-verification of risk is a key factor for a warning system. Self-verification of risk is the ability of the warning message recipient to make linkages between the warning message that is received and what he sees, hears or feels. A recipient uses the process of independent self-verification to formulate his perceived reality of the risk faced. In the case of a tornado warning, the message recipient after hearing the warning may not heed the warning until he can link the message to visual or physical cues. If the recipient sees dark skies and feels strong blowing winds, the likelihood that the message will be acted upon may be increased, whereas if the recipient sees clear skies and sunshine, it most likely will not. Thus warning systems must be able to adequately convey the risk message in sufficient detail to the recipient audience. The recipient must in turn not only hear the message but internalize it through the self-verification-of-risk process to form his unique risk reality. A properly designed warning system will provide sufficient informational elements as outlined in the risk-predictors and hazard-characteristics information sets to allow for this process. Each of the three warning systems detailed in this thesis (forest fire, tornado, and hurricane) carries

sufficient informational elements to allow the recipient to formulate his perceived reality of the risk. Perhaps this is one of the reasons why there is little criticism of these systems, unlike the HSAS system. The HSAS carries with it an insufficient number of information elements that can be use in the independent self-verification process to form a unique risk reality.

Past history of HSAS issuance has shown that threat levels have been raised after the fact (e.g., the first anniversary of 9/11, the United States attack against Iraq, the London mass-transit attacks). Thus, warnings have been issued for the possibility of attack or after-event onset, rather than for actual impending attack, an important difference from the other warning systems. This difference affects the social acceptance of the message and ultimately the internalization of the warning as a real danger. It is interesting to note here that in a report prepared for the Council for Excellence in Government, 62 percent of the American population stated that they found the HSAS useful, but when asked if they changed any part of their daily activity because of a threat level change, 84 percent responded that they did not (Council for Excellence in Government, 2004, p. 38). Might part of this lack of internalization of threat be attributable to the self-verification of risk process?

While there is little research documenting self-verification, it is highlighted in Quarantelli's 1990 work, *The Warning Process and the Evacuation Behavior: The Research Evidence*. In this work Quarantelli posits that the definition of the situation (the recipient's unique risk reality) intervenes between the intentions of those issuing what they believe are adequate warning messages and the perceptions and reactions of the intended recipients. Risk internalization is dependant on the belief that it is a warning and the confirmation of that belief (Quarantelli, 1990, p. 3). According to the National Weather Service's report on Mother's Day (May 10, 2008) weekend, tornado storm victims in post-event interviews stated that even though they were aware of the warnings, they did not feel personally at risk until they had visual or other confirmation of the threat (National Weather Service, 2009, p. 28).

In the case of forest fire prevention, the public can see the amount of ground cover and feel its moisture content, if so desired. The public is well aware when an area experiences a lack of moisture because of little or no rainfall; the public can see the browning of the trees and grasses within the forest. In the case of tornados, once a warning is issued, the public again can independently verify the possibility of the event since wind and rain are precursors of a tornado. Since tornados are spawned out of thunderstorms, there is a confirmation of the possibility of the event, even if no tornado is formed. Lastly, in hurricanes, rain, wind, and storm surge precede the main onset of the hurricane; thus, a visual verification of the event is available. In fact, for hurricanes this visual verification of the warning is generally available days before the actual hurricane's arrival. Thus, the key to the acceptance of these warning systems may be that they all carry a publicly verifiable component—a direct cause and effect relationship that cannot only be seen, but experienced. Additionally, these warnings are issued numerous times each year, so audiences readily see the pattern of warning issuance, followed by event onset, and ultimately warning cancellation because of threat subsidence. The threat that causes a change in the HSAS is not publicly verifiable, nor does it have a pattern of warning, followed by event onset, and ultimately event subsidence with cancellation of warning.

b. Negative Influences on Lack of Public Verification

Lack of public verification can also make the threat system seem susceptible to political factors that can corrupt the process. Secretary Ridge cited this possibility in his own book (Ridge, 2009, p. 237). Diana Bossio (2005), in her paper on the Australian threat system and its accompanying public awareness campaign, "Be Alert, Not Alarmed," writes

> Government communications often highlight state reliance on the operational discourse of threat and protection. The projections of fearful "Realities" are balanced with the state's evidence of its ability to control the unanticipated. Risks are strategically deployed at politically beneficial times to legitimize the actions of incumbent authorities. Government

> communications are produced to elicit social acceptance of these actions through the presentation of idealized narratives of individuals working within a collective national identity to defeat "Terror."

This same criticism has been raised numerous times within the last few years in the United States as well. John Paul and Sangyoub Park (2009) published a paper stating that terror threat systems allowed for potential political manipulation for political gain. This issue was also cited by Robb Willer in his paper, "Effects of Government-Issued Terror Warnings on Presidential Approval Ratings" (2004). The issue of political manipulation of terrorist threat warnings for political gain is an issue that has been cited numerous times in the press, both inside and outside of this country. It is mentioned here simply as a factor that has been reported in the literature as having the potential to impact negatively on the HSAS and cause the system to lose credibility, although this currently cannot be demonstrated to be the case.

In Chapter III, I will make a comparison of dissimilar threat systems to show that the HSAS does not contain enough of the informational elements as identified in the Oak Ridge National Laboratory study to allow it to adequately craft a warning message.

THIS PAGE INTENTIONALLY LEFT BLANK

III. ANALYSIS OF COMPARED WARNING SYSTEMS

The next part of the thesis will compare the three dissimilar threat systems against the HSAS in relation to how they measure up against the five factors for risk prediction and the six hazard characteristics as put forth in the Oak Ridge National Laboratory study. The results of this comparison will be used to assess whether the HSAS as designed provides the essential information elements to allow for the adequate preparation of an effective risk communication message. Important in this regard, as noted in Chapter II, is the ability of an audience to independently verify the risk information that a warning system provides.

A famous Sesame Street song by Joe Raposo, Jon Stone, and Bruce Hart, entitled, "One of These Things,"[6] posits that "one of these things is not like the others, one of these things just does not belong." Such is the problem that this thesis examines as related to the HSAS. This section looks at the similarities and the differences between forest-fire prevention, tornado, hurricane and terrorism threat warning systems. While all of the warning systems are seemingly different and unrelated, they do indeed share a commonality within the risk-communication arena, but the prediction of risk for terrorism, which is more art than science, may not contain enough informational elements within the risk predictors or hazard characteristic information sets to allow it to adequately craft a risk message.

As detailed in Chapter II, the study conducted by the Oak Ridge National Laboratory on warning systems in general provides insight as to why a warning system may or may not be effective. The report cited five factors significant for risk prediction and six items for hazard characteristics. The risk predictors were lead time, area of impact, magnitude, probability, and consequences. The study states that the purpose of these risk predictors is to forecast the behavior of the hazard in a way useful for providing a warning for the impending event (Mileti & Sorensen, 1990, pp. 2–6). For the

[6] "One of These Things," composed by Joe Raposo, Jon Stone, and Bruce Hart, © Sesame Street.

comparative purposes of this thesis, I will define parameters for the above-stated risk predictors and hazard characteristics so that a rational comparison can be made between the dissimilar warning systems.

A. RISK PREDICTION

1. Risk Prediction Defined

Since the study did not place parameters on the risk predictors, I have assigned the following definitions, which are in line with the study recommendations. Within the risk prediction category, *lead time* will be defined as either short, medium, long, or unknown. Short equates to a time frame of minutes to hours. Medium is hours to a day, and long is greater than a day. *Area of impact* will be categorized as either definable or indefinable. To be definable, an area of impact must be specifically locatable by use of accepted geographical coordinates (within a margin of error not to exceed 10 miles either side of a point or line). *Magnitude* is defined as uncertain or measurable. For a measurable magnitude, the event must be describable before onset according to an accepted scientific scale. *Probability* is defined as low (not likely to take place), medium (likely to take place), or high (almost certain to take place). The term *consequences* is defined as known if we can be certain of an impact upon a physical structure(s) or person(s) and unknown if we do not know whether there will be any impact upon a physical structure(s) or person(s).

2. Forest Fires

The threat warning system for forest fires is very specific and well defined. There are a number of very specific items that are factored into the models for prediction of unplanned ignitions. The main items are amount of ground cover, moisture content of ground cover, ambient air temperature, vapor pressure, and month of year (Vasilakos, Kalabokidis, Hatzopoulos, & Matsinos, 2008). In forest-fire warnings for unplanned ignitions, the forest is measured for the amount of ground cover loading and the moisture content within the ground cover. This is then coupled with the expected ambient air temperatures over the coming days and the expectation of rain. As the ground cover dries out due to heat (ambient air temperatures) and lack of moisture (rain), the forest increases

in susceptibility for an unplanned ignition. As we relate forest fires to the five factors of risk prediction, we can assign the descriptors defined above as follows:

Lead time: Long. We can predict conditions and their continued rate of either decline or improvement of ground cover susceptible to ignition based upon scientific modeling. (However, another variable such as a lighting strike, human intervention, or some other source of ignition must cause the event to begin.)

Area of impact: Definable. We can define the geographic limits of the forest according to accepted geographical coordinates.

Magnitude: Uncertain because there is no scientific gauge to measure magnitude before ignition.

Probability: Medium. Scientific measures have been made and can show that conditions are right for an unplanned ignition of the forest due to loading of ground cover, moisture content, ambient temperatures, and expectation of rain, but the actual ignition event (human or natural) is not as predictable.

Consequences: This is unknown because man can quickly intervene to extinguish the fire or the fire may not thrive due to other forces of nature.

3. Tornados

Tornados develop within supercells of thunderstorms. They begin with an interaction between an updraft and a larger-scale horizontal wind. It is this wind that exhibits strong vertical sheer in both speed and direction. As the wind speed increases with altitude and the wind direction veers (turns clockwise with altitude), the wind speed causes the air to rotate about a horizontal axis in a rolling motion; a tornado is formed (Moran & Morgan, 1997, p. 341). As we relate tornados to the five factors of risk prediction, we can assign the descriptors as follows:

Lead time: Short because tornados usually live on the ground for less than three minutes, and the lifetime of the thunderstorm system usually does not last longer than two hours (Moran & Morgan, 1997, p. 335).

Area of impact: Definable since we can define the geographic limits of the storm and predict its path with a level of certainty according to accepted geographical coordinates.

Magnitude: Uncertain. While there is a measure of intensity called the F-Scale, this is done after the event, based upon measurable wind speeds and damage assessments (Moran & Morgan, 1997, p. 340).

Probability: Medium for tornados. We can use radar to detect and track the path of thunderstorms and can gauge intensity. In some instances, radar can see a hook-shaped radar echo that tends to indicate rotational movement, which is a leading indicator of a tornado (Moran & Morgan, 1997, p. 347). Likewise a weather observer network is in place to watch severe thunderstorms and report actual tornado sightings.

Consequences: Known. Once a tornado is confirmed as being on the ground in relation to its geographical area, we can make judgments on its impact in the general direction of travel.

4. Hurricanes

Hurricanes form when tropical storms moving across the world's oceans find warm waters (>25 C) and at the same time encounter upper-air flows. It is these upper-air flows that help to pump out the storm's latent heat at the top faster than it can be replaced at the surface, thus intensifying the storm. This cycle encourages the influx of additional warm, moist air at the surface, which helps to intensify and sustain the hurricane (Lutgens & Tarbuck, 1982, p. 262). Hurricanes relate to the five factors of risk prediction as follows:

Lead time: Long. Hurricanes move east to west at about 25 kilometers an hour; when they turn poleward, their speed increases to a maximum of 100 kilometers per hour (Lutgens & Tarbuck, 1982, p. 262).

Area of impact: Definable. We can measure the speed and direction of a hurricane and we can define the geographic limits of the expected landfall according to accepted geographical coordinates.

Magnitude: Measurable, according to the scientifically accepted Saffir/Simpson scale (Lutgens & Tarbuck, 1982, p. 265).

Probability: High. Due to their slow movement and ability to be monitored, we can measure storm intensity and track its movement while it is still at sea. Landfall can be predicted almost with certainty.

Consequences: Known. We can measure the storm intensity well out at sea with a specific scale. We can also measure storm surge and predict levels of flooding based on known impact area land elevations.

5. Terrorism Threats

There is no single, universally accepted definition of terrorism. The definition used here is merely a point of reference to distinguish a terrorist act from a criminal act. Terrorism as defined in the Code of Federal Regulations is "the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives." (28 C.F.R. Section 0.85) Terrorism is related to the five factors of risk prediction as follows:

Lead time: Uncertain. In the past, some terrorist groups have provided advance notice of a pending attack, but this is not the norm.

Area of impact: Indefinable, unless a specific advanced warning was received.

Magnitude: Uncertain. No scientific scale is available for measurement

Probability: Low, unless specific information is received or intelligence makes a very specific intercept.

Consequences: Unknown until event onset.

6. Summation of Risk Prediction

The following chart summaries the risk prediction assigned to the four warning systems.

Table 2. Risk Prediction Summary

	Forest Fires	Tornados	Hurricanes	Terrorism Threats
Lead time	Long	Short	Long	Uncertain
Area of impact	Definable	Definable	Definable	Indefinable
Magnitude	Uncertain	Uncertain	Measurable	Uncertain
Probability	Medium	Medium	High	Low
Consequences	Unknown	Known	Known	Unknown

This chart serves as a summation of the ability of the several threat systems to predict risk. The more accurately a warning system can define a risk, the better its ability to allow for appropriate risk communication to the recipient audience. Without risk predictability, a warning system's ability to project the message in sufficient detail is lost. As cited earlier, for a threat system to be useful, it must provide the essential informational elements in sufficient quantity to allow the recipient not only to understand the nature of the threat, but also to internalize the risk. If recipients fail to internalize the risk, they often fail to heed the warning. For terrorism, only one of the risk predictors (probability) can be accurately classified, while the other systems examined can classify at least three risk predictors. As can also be seen in the chart, the first two predictors (lead time and area of impact) are both unknown within the terrorism arena. These two factors are the keys to allowing the recipient to undergo the independent self-verification-of-risk process; lead time and area of impact are the "when" and "where" of an event. If the risk communication message is to have any chance of being received and internalized by the audience, these two factors should be specified. The other three systems used in the comparison all supply these two factors. As noted, although the recipients may be aware of a threat, they often fail to internalize the threat until they receive a further confirmation of physical danger by way of visual, physical authentication or through social affirmation. Hence, a warning system that lacks an adequate number of risk predictors may never be able to meet the required level of specificity for this independent self-verification-of-risk process to take place and allow the recipients to form their own unique risk reality.

B. HAZARD CHARACTERISTICS

The Oak Ridge National Laboratory report defines six specific hazard characteristics that are required to define the hazard sufficiently to allow the proper crafting of a warning message. The report defines these hazard characteristics as follows:

1. Predictability: the ability to predict or forecast the impact of a hazard with respect to magnitude, location and timing;
2. Detectability: the ability to confirm the prediction that impacts are going to occur;
3. Certainty: the level of confidence that predictions and impacts are going to occur;
4. Lead time: the amount of time between prediction/detection and the impact of the hazard.;
5. Duration of impact: the amount of time between the beginning and the end of impact and the duration during which warnings can occur; and
6. Visibility: the degree to which the hazard physically manifests itself so that it can be seen or otherwise sensed (Mileti & Sorensen, 1990, p. 6-1).

These factors provide the risk-communication message with a higher level of specificity to allow individuals to receive the information they need to make informed, independent judgments about risk (unique risk reality). While the risk predictors give the “when,” “where,” and perhaps a sense of how bad, the hazard characteristics refine these into an appropriate sense of urgency for the message recipient. Each of the hazard characteristics has direct applicability and impacts upon one or more of the three basic components of a warning system (detection, emergency management, or public response) (Mileti & Sorensen, 1990, p. 6–1). The chart below details how these hazard characteristics fit into the basic components.

Table 3. Correlation of Hazard Characteristics to Warning System Components

Hazard Characteristics	Warning System Basic Components		Interaction with the Warning System Basic Component
	Detection	Public Response	
Predictability	√	√	Defines the area to be impacted
Detectability	√	√	Ability to be discovered Helps for internalization of the risk message
Certainty	√	√	Ability to predict an event
Lead time	√	√	Provides the "when" Helps for internalization of the risk message
Duration of impact		√ √	Provides the "how long" Helps for internalization of the risk message
Visibility	√	√ √	Ability to detect a risk Helps for internalization of the risk message

These hazard characteristics for detection allow for the risk message to state what to look for along with the "when." In public response, it provides the factors to be used for the internalization of the risk message, and it provides the details that the recipient may find useful for making linkages during the self-verification-of-risk process.

1. Hazard Characteristics Defined

For purposes of this thesis, these hazard characteristics will be defined as follows: *Predictability* is defined as a measurable quantifier by use of a predetermined scale or model (e.g., the National Fire Danger Rating System (National Wildfire Coordinating Group, 2002, p. 5)) or the ability to accurately forecast the movement (path) of the event; otherwise, it is to be listed as uncertain. *Detectability* is defined as the ability to be discovered before event onset. *Certainty* is defined as low (not likely to happen as predicted), moderate (likely to happen as predicted), or high (will happen as predicted). *Lead time* will be defined as either short, medium, long, or unknown. *Duration of impact*

is defined in terms of a definable time window for length of event from time of onset to conclusion, or classified as indefinable. *Visibility*, the last hazard characteristics, means whether the event can be seen before impact and is rated either yes or no.

2. Forest Fires

Predictability: Measurable. The U.S. Forest Service has developed specific models which measure the likelihood of unplanned ignition due to the factors stated above (National Wildfire Coordinating Group, 2002).

Detectability: Non-discoverable before ignition. Currently there is no way to pinpoint the exact place of an unplanned ignition within a forest.

Certainty: Moderate. If no other forces of nature enter to alter the current conditions, the likelihood of ignition remains probable, waiting for a source of ignition.

Lead Time: Long. We can predict conditions and their continued rate of either decline or improvement of ground cover susceptible to ignition based upon scientific modeling. (However, another variable such as a lighting strike, human intervention, or some other source of ignition must cause the event to begin.)

Duration of impact: Indefinable. Like "consequences" (as stated above in risk predictors), numerous factors by either man or nature or both can combine to limit or prolong duration.

Visibility: No. Before ignition, forest fires have no detectability and hence no visibility.

3. Tornados

Predictability: Measurable. The U.S. Weather Service, through modeling and the use of radar and storm watchers, can locate, track, and project a path of movement once the existence of the tornado is confirmed.

Detectability: Discoverable. Once confirmed, a tornado spends varying amounts of time on the ground, and its path can be predicted.

Certainty: Moderate. Once detected by radar or confirmed by human source as being on the ground, the path and movement of the tornado can be anticipated.

Lead Time: Short because tornados usually live on the ground for less than three minutes, and the lifetime of the thunderstorm system usually does not last longer than two hours (Moran & Morgan, 1997, p. 335).

Duration of Impact: Definable. Because of radar, we can track the accompanying thunderstorm and its speed; thus, we can not only predict arrival time at a given geographical point but can make a realistic estimate for length of time on target.

Visibility: Yes. A tornado can be seen approaching by both radar and the human eye.

4. Hurricanes

Predictability: Measurable. The U.S. Weather Service, through modeling and the use of radar, can locate and track not only the hurricane, but they can also project landfall location and time.

Detectability: Discoverable. Once identified, a hurricane can be tracked, plotted, and watched as it moves across the ocean days before it makes contact with land.

Certainty: High. Once detected by radar, the path and movement of a hurricane can be anticipated.

Lead Time: Long. Hurricanes move east to west at about 25 kilometers an hour; when they turn poleward, their speed increases to a maximum of 100 kilometers per hour (Lutgens & Tarbuck, 1982, p. 262).

Duration of impact: Definable. By means of radar, a hurricane can be tracked and its speed determined; the exact arrival time at a given geographical point along with a realistic estimate for length of time on target can be calculated.

Visibility: Yes. It can be observed days before land impact due to technology and human sightings.

5. Terrorism Threats

Predictability: Uncertain, unless specific information is received or intelligence makes a very specific intercept.

Detectability: Discoverable. Intelligence sources may uncover information of event onset, or a warning may be received.

Certainty: Low, unless specific information is made available by the sponsoring group.

Lead time: Uncertain. In the past, some terrorist groups have provided advance notice of a pending attack, but this is not the norm.

Duration of impact: Unknown. Weapon, means, and delivery system is generally unknown.

Visibility: No, not before event onset.

6. Summation of Hazard Characteristics

The chart below summarizes the ability of each threat system to adequately define the appropriate hazard characteristics. Terrorism threats are unable to adequately define the hazard characteristics, as was the case with the risk predictors. Terrorism allows adequate definition in two of the six hazard characteristics, while the others are able to define at least three. The key factors here are predictability and lead time—the “where” and the “when” an event will occur.

Table 4. Summary of Hazard Characteristics

	Forest Fires	Tornados	Hurricanes	Terrorism Threats
Predictability	Measurable	Measurable	Measurable	Uncertain
Detectability	Non-discoverable	Discoverable	Discoverable	Discoverable
Certainty	Moderate	Moderate	High	Low
Lead time	Unknown	Short	Long	Unknown
Duration of impact	Indefinable	Definable	Definable	Indefinable
Visibility	No	Yes	Yes	No

C. RISK PREDICTION AND HAZARD CHARACTERISTICS TABULATION

In order to be able to establish an overall effectiveness rating for each warning system regarding its ability not only to predict risk but to define the hazard in order to allow for the proper crafting of the risk message, I gave each positive predictor (i.e., measurable, definable) or hazard characteristic (i.e., measurable, discoverable) a numeric value of 1. If the predictor was not positive, it was assigned a numeric value of zero. Each system was then tallied to provide a comparison level of communication value.

Table 5. Numeric Tally of Risk Prediction and Hazard Characteristics

Risk Prediction				
	Forest Fires	**Tornados**	**Hurricanes**	**Terrorism Threats**
Lead time	1	1	1	0
Area of impact	1	1	1	0
Magnitude	0	0	1	0
Probability	1	1	1	1
Consequences	0	1	1	0
Hazard Characteristics				
	Forest Fires	**Tornados**	**Hurricanes**	**Terrorism Threats**
Predictability	1	1	1	0
Detectability	**0**	1	1	1
Certainty	1	1	1	1
Lead time	1	1	1	0
Duration of impact	0	1	1	0
Visibility	0	1	1	0
Tally	6	10	11	3

This numerical tally of risk predictors and hazard characteristics allows us to now answer the question of whether one of these warning systems is not like the others. As can be seen in the tally, three of the warning systems provide a level of specificity in their ability to communicate risk, as defined by the Oak Ridge National Laboratory study. Only the HSAS falls short in its ability to provide greater than fifty percent of the risk predictors or hazard characteristics needed to convey a risk message. Perhaps the HSAS as designed is not like the others and is not suitable to be an effective warning system.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. A RECOMMENDATION FOR THE SECRETARY OF HOMELAND SECURITY

This chapter outlines a recommendation for the Secretary of Homeland Security concerning the HSAS, along with some pros and cons associated with this recommendation. The recommendation is to rescind HSPD 3. While this may be the most prudent path, given the difficulties of creating an effective warning system for terrorism, it may be politically untenable. As has been shown, the HSAS since inception has been cloaked in controversy and criticism and is vulnerable to the appearance of political manipulation. While the concept of having a terrorism warning system to inform of dangers may sound good, the vehicle chosen to accomplish this task may have been flawed in its original development. The HSAS falls short of being a complete warning system. The HSAS lacks the ability to supply the essential elements required for effective risk predictors and hazard characteristics. This lack of essential elements undermines the audience’s ability to establish its own unique risk reality. If the audience is unable to form or underestimates its risk, it may not take the proper protective actions needed to counter a threat. The following recommendation details the reasons why the Secretary for Homeland Security should act upon this recommendation.

A. RECOMMENDATION

The Secretary of Homeland Security should urge the president to rescind Homeland Security Presidential Directive 3 and cease use of the HSAS. As has been shown, the HSAS does not supply a sufficient number of the informational elements for risk predictors and hazard characteristics as designated by the Oak Ridge National Laboratory report. The HSAS, by not supplying this information, fails to allow the audience to make the essential linkages between the warning message and its own visual/physical cues. This lack of specificity prevents audiences from undergoing the self-verification-of-risk process that is essential if they are to form their own risk reality. If the message recipients cannot form or underestimate their risk, they may fail to take the necessary precautions, which in turn negates the intended use of the warning system; thus, the HSAS cannot be an effective warning system.

As has been shown in this thesis, a warning system needs many informational elements to successfully craft a warning message. A terror threat warning system, by its nature, can never rise completely to this task because some of the essential informational elements will always remain unknowns; within the risk predictors information set, the elements of lead time, area of impact, (the "when" and "where"), and magnitude will always be ill-defined unless the organization carrying out the attack feels a need to forewarn. From the terrorist point of view, these two pieces are the elements of surprise that the terrorist organization needs for a successful operation; hence they tend to be the most closely guarded pieces of information. The third element within risk predictors is magnitude, which cannot be assessed because there cannot be a predefined scientific scale to premeasure the magnitude of a terrorist event before onset. Likewise, within the hazard characteristics informational sets, the elements of predictability, lead time, duration of impact, and visibility will always remain as unknowns. Predictability as defined within this thesis is a measurable quantifier by use of a predetermined scale or model, or the ability to accurately forecast movement (path) of the event. Terror events do not have such a scale, nor can the path of movement be predicted. Lead time, as mentioned in risk predictors, is the "when" and will not usually be known in terror attacks unless the sponsoring organization forewarns since if the "when" is known, law enforcement can make substantial efforts to prevent and/or disrupt before event onset. Duration of impact is defined in terms of a definable time window for length of event from time of onset to conclusion. Since terror attacks usually involve the use of explosives, the actual event is usually milliseconds; there have been other kinds of attacks that have lasted longer (e.g., 9/11 use of aircraft as missiles and the Mumbai swarming attack), but these are outside the usual pattern of circumstances. History has shown that the actual attack is very short, while the post-event response can be very prolonged and difficult. Visibility is the last element: that is, can the event be seen before its initial impact? In terror attacks, this element cannot be seen by audiences before event onset, unlike tornados and hurricanes. It is for these reasons that the secretary should urge the president to rescind HSPD-3.

1. Pros

- Frees the Department of Homeland Security of the responsibility of maintaining a marginal warning system.
- Lessens tensions between the various intelligence-gathering agencies as to the timing for public release of sensitive intelligence information.
- Removes the possibility that the Department of Homeland Security could be tainted by accusations that the HSAS threat levels were manipulated for political gain.
- The nation has sufficiently developed other communication methods that could be used to convey a serious and imminent threat message.

2. Cons

- Elimination of the HSAS conflicts with Executive Order 13407, which states: "It is the policy of the United States to have an effective, reliable, integrated, flexible, and comprehensive system to alert and warn the American people in situations of war, terrorist attack, natural disaster, or other hazards of public safety and well being."

Based upon the analysis conducted in Chapter III, it is not advisable for the secretary to attempt to revise the HSAS, either by requiring future threat increases to be issued for geo-specific locations or to be issued for a limited number of days, as various studies and governmental reports have called for. This type of revision would not significantly improve the nation's ability to communicate a terrorist threat. The HSAS's goal at inception was to create a general awareness of the challenges that the nation faced from terrorism and to provide a starting place for a national discussion on preparedness. In this it has been successful, but the nation has moved on to a new level of vigilance that surpasses the original intent of the HSAS. Coupled with the inability of the HSAS to craft a complete warning message, the current level of vigilance warrants rescinding the HSAS.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. THREAT CONDITIONS AND ASSOCIATED PROTECTIVE MEASURES

The world has changed since September 11, 2001. We remain a nation at risk to terrorist attacks, and we will remain at risk for the foreseeable future. At all levels of threat , we must remain vigilant, prepared, and ready to deter terrorist attacks. The following threat conditions each represent an increasing risk of terrorist attacks. Beneath each threat condition are some suggested protective measures, recognizing that the heads of federal departments and agencies are responsible for developing and implementing appropriate agency-specific protective measures:

A. LOW CONDITION (GREEN)

This condition is declared when there is a low risk of terrorist attacks. Federal departments and agencies should consider the following general measures in addition to the agency-specific protective measures they develop and implement:

- Refining and exercising as appropriate preplanned protective measures;
- Ensuring personnel receive proper training on the Homeland Security Advisory System and specific preplanned department or agency protective measures; and
- Institutionalizing a process to assure that all facilities and regulated sectors are regularly assessed for vulnerability to terrorist attack, and all reasonable measures are taken to mitigate these vulnerabilities.

B. GUARDED CONDITION (BLUE)

This condition is declared when there is a general risk of terrorist attacks. In addition to the protective measures taken under the previous threat condition, federal departments and agencies should consider the following general measures in addition to the agency-specific protective measures that they will develop and implement:

- Checking communications with designated emergency response or command locations;
- Reviewing and updating emergency response procedures; and
- Providing the public with any information that would strengthen its ability to act appropriately.

C. ELEVATED CONDITION (YELLOW)

An elevated condition is declared when there is a significant risk of terrorist attacks. In addition to the protective measures taken under the previous threat conditions, federal departments and agencies should consider the following general measures in addition to the protective measures that they will develop and implement:

- Increasing surveillance of critical locations;
- Coordinating emergency plans as appropriate with nearby jurisdictions;
- Assessing whether the precise characteristics of the threat require the further refinement of preplanned protective measures; and
- Implementing, as appropriate, contingency and emergency response plans.

D. HIGH CONDITION (ORANGE)

A high condition is declared when there is a high risk of terrorist attacks. In addition to the protective measures taken under the previous threat conditions, federal departments and agencies should consider the following general measures in addition to the agency-specific protective measures that they will develop and implement:

- Coordinating necessary security efforts with federal, state, and local law enforcement agencies or any National Guard or other appropriate armed forces organizations;
- Taking additional precautions at public events, and possibly considering alternative venues or even cancellation;
- Preparing to execute contingency procedures, such as moving to an alternate site or dispersing the workforce; and
- Restricting access to threatened facilities to essential personnel only.

E. SEVERE CONDITION (RED)

A severe condition reflects a severe risk of terrorist attacks. Under most circumstances, the protective measures for a severe condition are not intended to be sustained for substantial periods of time. In addition to the protective measures under the previous threat conditions, federal departments and agencies also should consider the following general measures in addition to the agency-specific protective measures that they will develop and implement:

- Increasing or redirecting personnel to address critical emergency needs;
- Assigning emergency response personnel and prepositioning and mobilizing specially trained teams or resources;
- Monitoring, redirecting, or constraining transportation systems; and
- Closing public and government facilities.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. HISTORY OF CHANGES IN THE THREAT ADVISORY LEVEL (DHS)

March 12, 2002	Introduction of the Homeland Security Advisory System; Initial threat level assigned is Yellow.
September 10, 2002	National level rises from Yellow to Orange; Possible anniversary attack on the United States for September 11; Lowered again to Yellow on September 24, 2002.
February 7, 2003	National level rises from Yellow to Orange; General terror threats against high occupancy buildings; Lowered again to Yellow on February 27, 2003
March 17, 2003	National level rises from Yellow to Orange in response to U.S. attacks against Iraq; Lowered again to Yellow on April 16, 2003.
May 20, 2003	National level rises from Yellow to Orange in response to attacks in Saudi Arabia and Morocco; Lowered again to Yellow on May 30, 2003.
December 21, 2003	National level rises from Yellow to Orange; Threats against the homeland centering on the Christmas holidays; Lowered again to Yellow on January 9, 2004.
August 1, 2004	Regional level rises from Yellow to Orange in New York City, northern New Jersey, and Washington, D.C. for just the financial sector; Intelligence threat against specific targets; Lowered again to Yellow on November 10, 2004.
July 7, 2005	Mass transportation sector only rises from Yellow to Orange; London mass-transit attacks; Lowered again to Yellow on August 12, 2005.
August 10, 2006	Air transportation sector only rises from Yellow to Red for flights inbound or outbound from the United Kingdom; Air transportation sector only rises from Yellow to Orange for all other commercial air traffic within the United States; Attempted bombing of an international aircraft; Lowered to Orange on August 13, 2006 on flights from the United Kingdom; all other air traffic within the United States remains at Orange.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

28 Code of Federal Regulations, Section 0.85 (definition of "terrorism"). Retrieved January 10, 2010 from http://www.fbi.gov/publications/terror/terror2000_2001.htm

Bossio, Diana. (2005). Be alert, not alarmed: Governmental communication of risk in an era of insecurity. Presented at the Annual Meeting of the Australian and New Zealand Communications Association, July 7–4, 2005.

Brooks, Harold E., & Doswell, Charles A. (2002). Deaths in the 3 May 1999 Oklahoma City tornado from a historical perspective. *American Meteorological Society* 17: 360.

Council for Excellence in Government. (2004). From the home front to the front lines: America speaks out about homeland security. Retrieved January 8, 2010 from ceg.files.cms-plus.com/EmergencyPreparedness/Homeland_Full_Report.pdf.

Faculty of Forestry and the Forest Environment, Lakehead University. Forest fire prediction and analysis. Retrieved January 8, 2010, from http://www.borealforest.org/world/innova/fire_prediction.htm.

Federal Bureau of Investigation. (2002). Homeland Security Alert System (HSAS) 45-day public comment period, e-mails and written comments from the public report of findings.

Gilmore Commission. (2003). Forging America's new normalcy: Securing our homeland, preserving our liberty. Fifth annual report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction.

Homeland Security Advisory System. (2009). Task force report and recommendations.

Homeland Security Presidential Directive 3. (2003). Homeland Security Advisory System, March 11, 2003.

Katsaros, K. B., Forde, E. B., Chang, P., & Liu, W. T. (2001). QuickSCAT's sea winds facilitates early identification of tropical depressions in 1999 hurricane season. *Geophysical Research Letters* 28:1043–46.

Klemp, Joseph P. (1987). Dynamics of tornadic thunderstorms. *Annual Review of Fluid Mechanics* 19: 369–402.

Lutgens, Frederick K., & Tarbuck, Edward J. (19820. *The atmosphere: An introduction to meteorology*. Englewood Cliffs, NJ: Prentice-Hall.

McLuckie. (1970). *The Warning System in Disaster Situations: A Selective Analysis.*

McQuillan, Patrick, Nye, Lindsey, Munoz, Amanda, Mendelson, Bradley. (2009). HSAC's HSAS Task Force, Summaries of HSAS Readings.

Mileti, Dennis S., & Sorensen, John H. (1990). Communication of emergency public warnings, a social science perspective and state-of-art assessment. Oak Ridge National Laboratory.

Moran, Joseph M., & Morgan, Michael D. (1997). *Meteorology, the atmosphere and the science of weather.* Upper Saddle River, NJ: Prentice Hall.

Morgan, M. Granger, Fischhoff, Baruch, Bostrom, Ann, Atman, Cynthia J. (2002). *Risk communication—A mental models approach*. Cambridge University Press.

National Wildfire Coordinating Group. (2002). Gaining an understanding of the national fire danger rating system.

National Weather Service. (2009). Mother's Day weekend tornado in Oklahoma and Missouri, May 10, 2008.

National Weather Service. National Fire Danger Rating System Description. Retrieved January 9, 2010 from http://www.wrh.noaa.gov/sew/fire/olm/nfdrs.htm

Paul, John, & Park, Sangyoub. (2009). With the best of intentions: The color coded Homeland Security Advisory System and the law of unintended consequences. Research and Practice in Social Sciences.

Perry, Ronald W., & Mushkatel, Alvin H. (1986). *Minority citizens in disaster.* University of Georgia Press.

Quarantelli, E. L. (1990). *The warning process and the evacuation behavior: The research evidence.* University of Delaware, Disaster Research Center.

Quarantelli, E. L., & Taylor, Verta A. (1977). *Some views on the warning problem as suggested by sociological research*. Ohio State University.

Ridge, Tom. (2009). *The test of our times.* Thomas Dunne Books.

Rogers, George O., & Sorensen, John H. (1993). *Diffusion of emergency warning: Comparing empirical and simulation results*. Oak Ridge National Laboratory.

Sharp, D., Blottman, P., & Troutman, T. (2000). Tornado warning situations for east central Florida. 20th Conference on Severe Local Storms, American Meteorological Society, Orlando, Florida.

Smith, Richard. (2000). Communicating the threat in warnings and statements: Call to action statements. National Weather Service Southern Region Headquarters, Meteorological Services Division, Technical Attachment: SR SSD 2000-12.

Smith, Richard D. & Piltz, Steven F. (1999). Situation specific tornado warnings at the National Weather Service Forecast Office, Tulsa, Oklahoma. *National Weather Digest* 23: 1–2, 41–44.

Tierney, Kathleen J., Lindell, Michael K., & Perry, Ronald W. (2001). *Facing the unexpected: Disaster preparedness and response in the United States.* Washington D.C.: Joseph Henry Press.

United States Department of Homeland Security. Chronology of changes to the Homeland Security Advisory System. Retrieved January 14, 2010, from http//:www.DHS.gov

United States Department of Homeland Security. (2003). Top Officials (Top Off) Exercise Series: Top Off 2, After Action Summary Report.

United States Department of Homeland Security. (2005). A review of the Top Officials 3 Exercise.

United States Department of Homeland Security. (2009). DHS efforts to address lessons learned in the aftermath of Top Officials Exercises.

United States General Accounting Office. (2004). Risk communication principles may assist in refinement of the Homeland Security Advisory System, GAO-04-538T. Washington D.C.

United States National Committee for the Decade for Natural Disaster Reduction, National Research Council. (1991). A safer future: Reducing the impacts of natural disasters. National Academies Press.

Vasilakos, Christos, Kalabokidis, Kostas, Hatzopoulos, John, & Matsinos, Ioannis. (2008, December 5). Identifying wildland fire ignition factors through sensitivity analysis of a neural network. *Journal of Natural Hazards.*

Willer, Robb. (2004). Effects of government-issued terror warnings on presidential approval ratings. *Current Research in Social Psychology*.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Janet Napolitano
   Secretary
   Department of Homeland Security
   Washington, D.C.